

SENATE BILL REPORT

SB 6281

As of January 22, 2020

Title: An act relating to the management and oversight of personal data.

Brief Description: Concerning the management and oversight of personal data.

Sponsors: Senators Carlyle, Nguyen, Rivers, Short, Sheldon, Wellman, Lovelett, Das, Van De Wege, Billig, Randall, Pedersen, Dhingra, Hunt, Salomon, Liias, Mullet, Wilson, C., Frockt, Cleveland and Keiser.

Brief History:

Committee Activity: Environment, Energy & Technology: 1/15/20.

Brief Summary of Bill

- Provides Washington residents with the consumer personal data rights of access, correction, deletion, data portability, and opt out of the processing of personal data for specified purposes.
- Specifies the thresholds a business must satisfy for the requirements set forth in this act to apply.
- Identifies certain controller responsibilities such as transparency, purpose specification, and data minimization.
- Requires controllers to conduct data protection assessments under certain conditions.
- Authorizes enforcement exclusively by the attorney general.
- Provides a regulatory framework for the commercial use of facial recognition services such as testing, training, and disclosure requirements.

SENATE COMMITTEE ON ENVIRONMENT, ENERGY & TECHNOLOGY

Staff: Angela Kleis (786-7469)

Background: The Federal Trade Commission (FTC) has been the chief federal agency on privacy policy and enforcement since the 1970s when it began enforcing the Fair Credit Reporting Act, one of the first federal privacy laws. The FTC uses its broad authority to

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

prohibit unfair and deceptive practices, but also enforces more specific privacy statutes, such as the Gramm-Leach Bliley Act and the Children's Online Privacy Protection Act.

Personal information and privacy interests are protected under various provisions of state law. The Washington State Constitution provides that no person is disturbed in their private affairs without authority of law.

The Consolidated Technology Services (CTS) agency supports state agencies as a centralized provider and procurer of information technology services. Within CTS, the Office of the Chief Information Officer (OCIO) has primary duties related to information technology for state government, which include establishing statewide enterprise architecture and standards for consistent and efficient operation. Within the OCIO, the Office of Privacy and Data Protection (OPDP) serves as a central point of contact for state agencies on policy matters involving data privacy and data protection.

Summary of Bill: Short Title. This act is known as the Washington Privacy Act.

Jurisdictional Scope. This act applies to legal entities conducting business in Washington or producing products or services targeted to Washington residents, and:

- controlling or processing personal data of 100,000 or more consumers; or
- deriving 50 percent of gross revenue from the sale of personal data and processing or controlling personal data of 25,000 or more consumers.

This act does not apply to local and state governments, municipal corporations, personal data regulated by certain federal and state laws, or data maintained for employment records purposes.

Responsibility According to Role. Controllers and processors are responsible for meeting set obligations. Processors must adhere to instructions of the controller and assist controllers in meeting set obligations. Notwithstanding the instructions of the controller, processors must implement reasonable security procedures, ensure the confidentiality of the processing of personal data, and engage with a subcontractor only after certain requirements are met.

Processing by a processor is governed by a contract between the controller and the processor that is binding on both parties and that sets out the processing instructions to which the processor is bound.

Consumer Personal Data Rights. *Consumer Rights.* Except as provided in this act, a consumer has the following rights:

- access—confirm whether a controller is processing their personal data and access such data;
- correction—correct inaccurate personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data;
- deletion—delete their personal data;
- data portability—obtain their personal data, which they previously provided to the controller, in a format that allows the consumer to transmit the data to another controller; and

- opt out—opt out of the processing of their personal data for purposes of targeted advertising, the sale of personal data, or profiling in furtherance of decisions that produce legal effects concerning a consumer or similarly significant effects concerning a consumer.

In the case of processing of personal data concerning a known child, the parent or legal guardian of the known child shall exercise these rights on the child's behalf.

Notifying Third Parties. A controller must, upon request, take reasonable steps to communicate a consumer's request to correct, delete, or opt out of the processing of personal data to each third party to whom the controller disclosed the personal data within one year preceding the consumer's request, unless this proves functionally impractical or involves disproportionate effort.

Responding to Consumer Requests. A controller must inform a consumer of any action, including an extension, taken on a request within 45 days of receipt of a request. This timeframe may be extended once for an additional 45 days. If a controller does not take action on a request, the controller must inform the consumer within 30 days of receipt of the request with the reasons for not taking action and instructions on how to appeal the decision with the controller. Controllers must establish an internal process for consumers to appeal a refusal to take action.

Information must be provided by the controller free of charge, up to twice annually, to the consumer. When requests from a consumer are manifestly unfounded or excessive, the controllers may either charge a reasonable administrative fee or refuse to act on the request. The controller bears the burden of demonstrating the manifestly unfounded or excessive character of the request.

A controller is not required to comply with a request to exercise a consumer personal data right if the controller is unable to authenticate the request using commercially reasonable efforts. In such cases, the controller may request additional information.

Processing Deidentified Data or Pseudonymous Data. Controllers or processors are not required to take certain actions in order to comply with this act, such as reidentifying deidentified data or maintaining data in an identified form. The consumer rights identified in this act do not apply to pseudonymous data in cases where the controller is able to demonstrate that it is not in a position to identify the consumer. A controller or processor that uses deidentified data or pseudonymous data must monitor compliance with any contractual commitments.

Responsibilities of Controllers. Controllers responsibilities include:

- providing consumers with a meaningful privacy notice that meets certain requirements, such as including instructions on how to exercise the consumer rights of this act;
- limiting the collection of personal data to what is required for a specified purpose as disclosed to the consumer;
- limiting the collection of data to what is relevant to a specified purpose as disclosed to the consumer;

- prohibiting processing for purposes not compatible with a specified purpose as disclosed to a consumer;
- establishing and implementing data security practices;
- prohibiting processing which violates state or federal law and discriminating against a consumer for exercising any of the consumer rights of this act; and
- obtaining consumer consent in order to process sensitive data.

Data Protection Assessments. Controllers must conduct a data protection assessment (assessment) of each of their processing activities involving personal data and any time there is a change in processing that materially increases the risk to consumers. Assessments must identify and weigh the benefits of the processing against the potential risks to the rights of the consumer associated with the processing. If the assessment determines the potential risks to the rights of the consumer outweigh the benefits of the processing, the controller may only engage in the processing with the consent of the consumer. Consent shall be as easy to withdraw as to give.

The attorney general (AG) may request, in writing, that a controller disclose any assessment relevant to an investigation conducted by the AG. The AG may evaluate the assessment with the controller responsibilities and with other laws. Assessments are confidential and exempt from public inspection.

Limitations and Applicability. Several exemptions to the obligations imposed on controllers or processors are specified such as complying with federal, state, or local laws, providing a service specifically requested by a consumer, or conducting internal research.

Personal data that is processed by a controller pursuant to an exemption must not be processed for any other purpose than those expressly listed. Personal data processed pursuant to an exemption may be processed solely to the extent that such processing is proportionate and limited to what is necessary in relation to a specified purpose. If a controller processes personal data pursuant to an exemption, the controller bears the burden of demonstrating that such processing qualifies for the exemption and complies with specified requirements.

Liability. Any violation shall not serve as the basis for, or be subject to, a private right of action under this act or under any other law.

Enforcement. The AG has exclusive enforcement authority. Any controller or processor that violates this act is subject to an injunction and liable for a civil penalty of not more than \$7,500 for each violation. The Consumer Privacy Account is created. All receipts from the imposition of civil penalties, except for the recovery of costs and attorneys' fees accrued during enforcement, must be deposited into the Consumer Privacy Account. Expenditures from the account may only be used for the purposes of the OPDP.

Preemption. This act supersedes and preempts laws, ordinances, regulations, or the equivalent adopted by any local entity regarding the processing of personal data by controllers or processors.

Reports and Joint Research Initiatives. The OPDP must conduct a study on the development of global opt out technologies and submit a report of its findings and recommendations to the Governor and the Legislature by October 31, 2021.

The AG must evaluate the liability and enforcement provisions and submit a report of its finding and recommendations to the Governor and the Legislature by July 1, 2022.

The Governor may enter into agreements with British Columbia, California, and Oregon to share personal data for joint research initiatives. Such agreements must provide reciprocal protections that the respective governments agree appropriately safeguard the data.

Commercial Facial Recognition Services. Processors that provide facial recognition services (services) must make available an application programming interface to enable independent tests of the service for accuracy and unfair performance differences across distinct subpopulations. If results of the independent testing identify material unfair performance difference across subpopulations and those results are validated, then the provider must develop and implement a plan to address the identified performance differences.

Processors that provide services must also provide documentation that includes specific general information and prohibits, in the required contract, the use of a service by controllers to unlawfully discriminate under federal or state law.

Controllers must provide a conspicuous and contextually appropriate notice that meets certain minimum requirements and obtain consumer consent prior to enrolling a consumer's image in a service used in a physical premise open to the public. A controller may enroll a consumer's image in a service without first obtaining consent from that consumer if certain requirements are met, such as the controller must hold reasonable suspicion, based on a specific incident, that the consumer has engaged in criminal activity.

Controllers using a service to make decisions that produce legal effects on consumers must ensure that those decisions are subject to meaningful human review.

Controllers shall not knowingly disclose personal data obtained from a service to law enforcement except when such disclosure is

- pursuant to consumer consent;
- required by law;
- necessary to prevent or respond to an emergency; or
- to the National Center for Missing and Exploited Children.

Controllers and processors deploying services must respond to a consumer request to exercise the consumer personal data rights and fulfill controller responsibilities.

Effective Dates. The effective date is July 31, 2021, except the section regarding the OPDP study takes effect 90 days after enactment.

Appropriation: None.

Fiscal Note: Available.

Creates Committee/Commission/Task Force that includes Legislative members: No.

Effective Date: The effective date is July 31, 2021, except the section regarding the OPDP study, which takes effect 90 days after enactment.

Staff Summary of Public Testimony: PRO: This takes the best elements from international and other state privacy laws and customizes them in a responsible way for Washington. Washington could be the model for data privacy laws for the nation. Consumers have the right to know what companies are doing with their personal data and companies should have certain obligations regarding that data. This bill is an opportunity to provide protections that do not exist today.

CON: The facial recognition regulations of this bill do not adequately protect Washington residents, and there needs to be a moratorium on the use of the technology. The communities that are most impacted by the use of facial recognition technology should be able to decide if it should be used. This technology should not be used for decisions that have legal effects. In order to provide the best protections to consumers, this bill needs to have a private right of action as well as increased resources to the attorney general. We think the definition of public information should include photos taken in public places.

OTHER: Although we understand the need to protect consumer personal data, we would prefer a federal data privacy law rather than a patchwork of state privacy laws. We have concerns with the definitions of deidentified data and sale. It would be helpful if there was a method of measurement with regards to thresholds for the scope of the bill. The Gramm-Leach Bliley Act exemption should be absolute. The requirement to notify the attorney general of all appeals may be burdensome. The loyalty program provisions are problematic; we will provide amendments. Local government should be able to pass laws regarding consumer privacy. We believe facial recognition should be addressed in a separate bill. The facial recognition regulations make it seem as though law enforcement is something that people need to be protected from.

Persons Testifying: PRO: Senator Reuven Carlyle, Prime Sponsor; Alison Phelan, BECU; Joe Adamack, Northwest Credit Union Association; Ryan Harkins, Microsoft.

CON: Cameron Cantrell, University of Washington School of Law; Jevan Hutson, University of Washington School of Law; Jennifer Lee, ACLU of Washington; Mark Streuli, Motorola Solutions; Neil Beaver, Washington Defenders Association and Washington Association of Criminal Defense Lawyers.

OTHER: Michael Schutzler, CEO, WTIA; Mark Johnson, Washington Retail Association; Eric Ellman, Consumer Data Industry Association; Bill Ronhaar, Washington Land Title Association; Stuart Halsan, Washington Land Title Association; Larry Shannon, Washington State Association for Justice; Trent House, Washington Bankers Association; Samantha Kersul, executive director Washington and the Northwest, TechNet; Justin Brookman, Consumer Reports; Andrew Kingman, general counsel, State Privacy & Security Coalition, senior managing attorney, DLA Piper; Rick Gardner, corporate counsel, LexisNexis Risk Solutions; James McMahan, Washington Association of Sheriffs and Police Chiefs; Rose Felciano, Internet Association; Fielding Greaves, Advanced Medical Technology

Association; Robert Battles, Association of Washington Businesses; Julia Gorton, Washington Hospitality Association; Andrea Alegrett, Attorney General's Office.

Persons Signed In To Testify But Not Testifying: No one.